Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Verfasser/in

Tilman Herbrich

Datum des Dokuments

01. August 2024

Ansprechpartner/in:

Dr. Mira Suleimenova

Projekt:

Datenschutzrechtliche Beurteilung der Kernkomponenten der JENTIS Software as a Service (SaaS) Lösung

Executive Summary

Die JENTIS GmbH („**JENTIS**“) begehrt eine Einschätzung für die datenschutzrechtliche Beurteilung der Kernkomponenten der JENTIS Data Capture Platform („**DCP**“).

Die JENTIS DCP bietet als Privacy Enhancing Technology eine nachhaltige Lösung zur Sicherstellung der Datenqualität, der vollständigen Kontrolle über die eigenen First-Party-Daten sowie der „Datenschutz“-Compliance in der Supply Chain und ermöglicht den Kunden flexible Konfigurationen der Server-Side-Tracking-Lösung, um der Volatilität der jeweiligen individuellen Risikolage von Unternehmen Rechnung zu tragen **(A.)**.

Das vorliegende Memorandum erläutert das nach Gesetzeslage, Behördenpraxis und Rechtsprechung rechtliche Anforderungsprofil an die Erfassung von Tracking-Daten von Consented- und Non-Consented-Nutzern sowie an die Weitergabe von Datenpunkten an Drittanbieter-Systemen für die Nutzung Analyse- und Marketing-Funktionalitäten und skizziert die zu ergreifenden Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus **(B.I.)**. Insbesondere bietet JENTIS mit dem JENTIS Essential Mode als Fall-Back-Lösung eine Möglichkeit, bei nicht gegebener Einwilligung Nutzer-Daten auf ein Mindestmaß zu reduzieren, sodass in Abhängigkeit der Risikoaffinität von Unternehmen Ausnahmen vom Einwilligungserfordernis für eine vollständige Reichweitenmessung belastet werden können **(B.I.3.)**.

Individuelle Konfigurationsmöglichkeiten ermöglichen die Gewährleistung einer Datenschutz-Compliance durch Umsetzung der Anforderungen nach Maßgabe des Europäischen Datenschutzausschusses („**EDSA**“) an Privacy by Design und Privacy by Default **(B.II.1.)**.

Bei Nutzung der JENTIS DCP kann durchgehend die TCF v2.2-Compliance beim Einsatz von zertifizierten Analyse- und Marketing-Tools sichergestellt werden **(B.II.2.).**

Für den Fall der Nutzung von Drittanbieter-Diensten aus einem Drittland ohne Angemessenheitsbeschluss der EU-Kommissionen oder potenziellen Weiterleitungen aus den USA in entsprechende Drittländer wie beim Einsatz von Google DV 360 lässt sich mithilfe der JENTIS DCP eine Synthetisierung der Datenparameter des Nutzers als wirksames Mittel der Pseudonymisierung nach Maßgabe der Empfehlungen des EDSA sicherstellen. Die Durchführung einer validen Pseudonymisierung ist als technische Mitigation etwaiger Zugriffsrisiken von Sicherheitsbehörden im Rahmen der Durchführung eines „Transfer Impact Assessments“ nach Ziff. 14 der Standardvertragsklauseln zu qualifizieren **(B.II.3.)**.

Best Practices für Unternehmen dienen als Handlungsempfehlungen für den rechtskonformen Einsatz der JENTIS DCP, die in Form einer Checkliste ausgestaltet sind **(B.III.)**.

Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Inhaltsverzeichnis

Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

A. Sachverhalt

(1) JENTIS bietet mit der Data Capture Platform („**DCP**“) eine in Deutschland oder wahlweise in Europa gehostete, mehrkomponentige, serverseitige Tracking-Technologie an, mit deren Hilfe die Datenqualität signifikant gesteigert und hochwertige First-Party-Daten erfasst werden können. Die Steigerung der Datenqualität wird dadurch bewirkt, dass Daten von Website-Nutzern in einem **First-Party-Kontext** ungeachtet von Ad-Blockern und Tracking-Schutzmechanismen[1] in Drittanbieter-Systemen wie Google Analytics oder Adobe Analytics mithilfe einer einzigartigen **Server-Side-Tracking-Technologie** verarbeitet werden können.

(2) Die JENTIS DCP bietet **drei** wesentliche **Vorteile**:

- **Qualität:** Die JENTIS DCP ermöglicht Marketing-Teams eine effizientere Budgetzuweisung, eine höhere Kampagnenrentabilität und einen verbesserten Return on Investment für Marketing-Kampagnen, da sie den Datenschutz durch Privacy by Design und Konfigurationsoptionen ermöglicht. Die JENTIS DCP orchestriert die Daten, indem es den Prozess der Datenerfassung,, -verwaltung und des sinnvollen Datenaustauschs mit Dritten vereinfacht und so effiziente Arbeitsabläufe fördert..
- **Controls:** Mit der JENTIS DCP gewinnen Website-Betreiber die Kontrolle bei der Erfassung von eigenen Datenpunkten der Nutzer zurück. Es können Daten vollumfänglich von solchen Nutzern, die eine Einwilligung erteilt haben, aber auch in verringertem Umfang von solchen Nutzern, die eine Einwilligung abgelehnt haben, im Einklang mit den Datenschutzvorgaben verarbeitet werden. Die JENTIS DCP lässt sich kundenspezifisch konfigurieren und auf individuelle Bedürfnisse anpassen.
- **Privacy Enhancing:**
    - Die JENTIS DCP ermöglicht einen **rechtssicheren Umgang** bei der Einbindung von Drittanbieter-Analyse- und Marketing-Diensten. JENTIS bietet die technische Möglichkeit, bestimmte, vom Website-Betreiber im First-Party-Kontext gewählte Daten an JENTIS-Server zu streamen und von dort aus an verschiedene andere Datenempfänger zu übermitteln, so dass der Website-Betreiber die Möglichkeit hat, die Datenlieferkette direkt zu beeinflussen und die Daten seiner Nutzer zu schützen.
    - Die JENTIS DCP ermöglicht mithilfe eines **serverseitigen Tagging** eine reduzierende und substituierende Filterung von Datenströmen, bevor diese an Drittanbieter wie Google oder Facebook weitergeleitet werden. Beim Einsatz der JENTIS DCP werden im Quellcode der Website implementierte Third-Party-Tags wie JavaScripte, iFrames und Image-Pixel derart modifiziert, dass weder ein unmittelbarer Endgerätezugriff noch eine unmittelbare Übermittlung von Nutzerdaten wie der IP-Adresse und User-IDs im Rahmen einer unmittelbaren Serveranfrage des Browsers des Nutzers an Drittanbieter-Server erfolgt. Eine direkte Verbindung zwischen dem Browser des Nutzers und der Drittanbieter wird auf diesem Wege von vornherein vermieden.
    - Die JENTIS DCP ermöglicht eine **Synthetisierung** von Nutzer-Daten. Synthetische Daten auf grundlegender Ebene sind künstlich erzeugte Daten, die aus den Originaldaten erzeugt werden und die statistischen Eigenschaften dieser Originaldaten bewahren, ohne jedoch einen Bezug zu einer identifizierten oder identifizierbaren Person aufzuweisen.[2]

[1] Z. B. ITP des Browsers Safari und ETP von Firefox.
[2] EDPS, techsonar 2021-2022, S. 10; López/Elbil, European Law Blog, On synthetic data: a brief introduction, 2022.

(5) Mithilfe der JENTIS DCP kann der von Google angekündigten Third-Party-Cookie phase-out wirkungsvoll ohne Reichweitenverluste begegnet werden. Für die in Zukunft notwendige Erfassung, Aufbereitung und Aktivierung von First-Party-Daten in Werbeökosystemen als wichtigste Weichenstellung für ein erfolgreiches Online-Marketing bietet JENTIS mit Utiq als deterministische und persistente ID-Solution eine rechtskonforme und valide Partnerschaft zur Monetarisierung von Daten und deren Attribution zur Erfolgsmessung von Werbekampagnen.[3]

(6) Die Kernelemente der JENTIS SaaS-Lösung umfassen folgende Systembestandteile der Produktbeschreibung und Systemarchitektur (siehe die Anhänge unten):

- JENTIS Container Manager und Tag Manager
- JENTIS Consent Manager
    - Inklusive Essential Mode
- JENTIS Tool Connector
- JENTIS Tracker
- JENTIS Server Suite und Twin Server

(7) JENTIS verarbeitet Nutzerdaten weisungsgebunden im Auftrag und nach Maßgabe der vom Website-Betreiber vorgenommenen Konfiguration der Verarbeitungssysteme und verarbeitet keinerlei Nutzerdaten zu eigenen Zwecken. JENTIS stellt einen Auftragsverarbeitungsvertrag im Einklang mit Art. 28 DSGVO bereit.

(8) Kein Gegenstand der vorliegenden Bewertung sind zusätzliche und erweiterte Features der JENTIS SaaS-Lösung sowie Aspekte der IT-Sicherheit.

B. Rechtliche Analyse

(1) Angesichts unzureichender Branchenlösungen für das Server-Side-Tracking und fehlender Praktikabilität, die von Aufsichtsbehörden mitgeteilten Anforderungen an eine ausdrückliche Einwilligung für den Drittlandtransfer zu erfüllen **(I.)**, wächst das Bedürfnis nach langfristigen und nachhaltigen Strategien zur rechtskonformen und erfolgreichen Datennutzung von Drittanbietern mit globalen Infrastrukturen.

(2) Eine Lösung für die Verflechtungen und Risiken im Bereich des Website-Tracking stellen Middleware-Konzepte wie die JENTIS SaaS-Lösung dar. **JENTIS** ermöglicht eine **flexible Konfiguration** der SaaS-Lösung, um der Volatilität der jeweiligen **individuellen Risikolage** von Unternehmen Rechnung zu tragen. Auf diesem Wege versetzt die JENTIS-Twin-Server-Technologie Unternehmen beim Einsatz von Tracking-Technologien von Drittanbietern in die Lage, die rechtlichen **Anforderungen** in der **Supply Chain sicherzustellen (II.).**

I. Datenschutzrechtliche Einordnung des Tracking über die JENTIS DCP

1. Möglichkeiten der Datenerfassung über JENTIS DCP

JENTIS hat sich auf das 1st Party Data Capturing mittels serverseitigen Tracking spezialisiert, welches Datenschutz und Tracking auf einer einzigen Plattform integriert. Die Lösung ersetzt dabei herkömmliche

[3] Vgl. Whitepaper. Beyond the 3rd Party Cookie. Die Revolution der Marketing-Infrastruktur. S. 4 ff.

Tag-Management-Systeme, indem User Sessions serverseitig gespiegelt werden (Twin-Browser-Technologie). Das ermöglicht es Unternehmen, Daten rechtskonform zu erfassen, aufzubereiten und mit diversen Marketing- und Analysetools zu integrieren, wodurch Marketer und Analysten hochwertige Daten aus verschiedenen Kanälen (wie unterschiedlichen Websites oder E-Commerce-Shops) erfassen und in ihren bestehenden Systemen nutzen können. Durch die Fähigkeit, Ad-Blocker und Tracking Preventions zu negieren, kann zudem der Datenumfang erhöht werden. Die vollständige Kontrolle über die Daten verbleibt dabei stets beim Unternehmen, was eine neue Ebene der Datenhoheit eröffnet.

a) JENTIS Container und Tag Manager

(1) Mit dem JENTIS Container wird sichergestellt, dass für jeden Kunden ein eigenständiges System zur Verfügung gestellt und keinerlei Verknüpfung mit anderen Kunden besteht. Der JENTIS Tag Manager ist ein System, das eine Orchestrierung der Tags von Drittanbieter-Systemen und das strukturierte Laden in Abhängigkeit der Nutzerpräferenzen bei Auswahl in dem Consent-Managament-Plattform („**CMP**“) sicherstellt. Je nach Kundenkonfiguration des Tag-Management-Systems kann der JENTIS Tag Manager entweder synchron mit der CMP geladen oder asynchron erst nach Erteilung einer Einwilligung geladen werden.

(2) Der JENTIS Container und der JENTIS Tag Manager wird aufgrund der Implementierung eines Skripts in eine Website beim Aufruf der Website per Default parallel, d. h. synchron zur JENTIS CMP (vgl. Pkt. I. 2.b.), geladen. Durch das Laden des Tag-Management-Systems wird die spätere Aktivierung und Verwaltung weiterer Programmcodes bei Erteilung einer Einwilligung der Nutzer ermöglicht. Ohne Erteilung einer Einwilligung der Nutzer findet keine gesonderte Speicherung von Nutzer-IDs oder ein zielgerichteter Zugriff auf das Endgerät statt.

Außerdem erlaubt der JENTIS Container und JENTIS Tag Manager die Datenparameter der Nutzer in einer bestimmten Reihenfolge auszutauschen, insbesondere durch Ordnung und Systematisierung der Datenpakete.

Für das Laden des JENTIS Container und JENTIS Tag Manager wird von dem Browser eines Nutzers eine https-Anfrage an die Domäne des Web-Servers gesendet und dabei die IP-Adresse des Nutzers sowie System- und Browserinformationen an den Website-Betreiber übermittelt.

(3) Das Laden des JENTIS Containers und JENTIS Tag Managers in der Serverantwort kann vorbehaltlich einer anderslautenden Rechtsprechung auf die Ausnahmeregelung in § 25 Abs. 2 Nr. 1 TDDDG gestützt werden (vgl. Pkt. B. I. 3. a.). Der JENTIS Container und JENTIS Tag Manager dient der Leitung von Informationen und dem Austausch von Datenelementen in einer vorgesehenen Reihenfolge – nämlich der Aktivierung weiterer Tags in Abhängigkeit der vorgenommenen Nutzerpräferenzen in der angeschlossenen CMP.

(4) Im Vergleich zu anderen Tag-Management-Systemen besteht bei Nutzung des JENTIS Tag Managers kein Infrastruktur-Risiko mit erhöhten Hürden für die Rechtfertigung wie bei Nutzung des Server Side Google Tag Managers. Denn bei Nutzung des Server Side Google Tag Managers wird der gesamte Tech Stack des Unternehmens in der Google Cloud Platform eingebettet. Damit geht auch für unkritische Tracking-Dienste mit reiner EU-Infrastruktur ein Verlust der Kontrolle über den Zugriff auf Nutzerdaten einher.[4]

[4] Vgl. Mertens/Bielova/Roca/Santos et. al., Google Tag Manager: Hidden Data Leaks and its Potential Violations under EU Data Protection Law.

Auch wenn der Server Side Google Tag Manager nicht in der Google Cloud Platform gehostet wird, müssen überdies die Regelungen für den Drittlandtransfer nicht nur in die USA beachtet werden (vgl. Pkt. II. 4.).

b) JENTIS Tracker, JENTIS Server Suite und JENTIS Twin Server

(1) Mithilfe der JENTIS Tracker können Website-Betreiber First-Party-Daten auf Basis der Tracking-Konfiguration im JENTIS Tracker über Cookies im First-Party-Kontext erfassen und serverseitig an die JENTIS Server Suite pushen. Die Speicherdauer der JENTIS Cookies kann individuell festgelegt werden.

(2) Die JENTIS Server Suite ist das Rückgrat der JENTIS SaaS. JENTIS verarbeitet die Daten ausschließlich auf dokumentierte Weisung nach Maßgabe der Konfiguration der JENTIS Server Suite durch den Website-Betreiber. Mit den Standard- und erweiterten Funktionen der JENTIS Server Suite können Website-Betreiber Nutzer modifizieren (anonymisieren und pseudonymisieren), anreichern und/oder synthetisieren, bevor sie an Drittanbietersysteme weitergeleitet werden. Die JENTIS Server Suite basiert auf der Twin Server Technologie. Der JENTIS Twin Server ist ein integraler Bestandteil der JENTIS Server Suite. Durch Duplikation der Serveranfrage aus dem Browser eines Nutzers können Datenpunkte vollständig entfernt, gefiltert, durch Modifikation verändert oder mittels Synthetisierung durch künstliche Werte ersetzt werden. Die Original-Server-Anfrage kann entweder vollständig gelöscht oder beibehalten werden.

Nachdem die Nutzerdaten aus der Serveranfrage verarbeitet, angereichert, substituiert, modifiziert oder synthetisiert wurden, können sie von der JENTIS Server Suite aus an Drittanbieter-Systeme wie Google Analytics gestreamt werden.

(3) Website-Betreiber können den Umfang der Verarbeitung durch individuelle Konfiguration der JENTIS Server Suite den eigenen Bedürfnissen und den rechtlichen Anforderungen selbständig anpassen. So können Nutzerdaten im Einklang mit den Anforderungen an die Abfrage einer rechtskonformen Einwilligung von Consented Nutzern **(I.2.)** oder/und im reduzierten und modifizierten Umfang nach Maßgabe des Features Essential Mode ohne Abfrage einer Einwilligung – gestützt auf die Ausnahmeregelung in § 25 Abs. 2 TDDDG –von Non-Consented Nutzern **(I.3.)** verarbeitet werden.

Die Weitergabe der substituierten Datenströme an Drittanbieter-Systeme kann bei Durchführung einer dokumentierten Interessenabwägung auf die Rechtsgrundlage gemäß Art. 6 Abs. 1 lit. f) DSGVO als der dem Endgerätezugriff nachgelagerten Verarbeitung gestützt werden **(I.4.)**.

2. Datenerfassung von Consented Nutzern

a) Einwilligungserfordernis für Endgerätezugriff bei Tracking zu Analyse- und Marketingzwecken

(1) Das Einwilligungserfordernis nach Art. 5 Abs. 3 S. 2 ePrivacy-RL (§ 25 Abs. 1 TDDDG in Deutschland) gilt für jeden Zugriff auf und jede Speicherung von Informationen aus Endgeräten der Nutzer – unabhängig davon, ob der Zugriff im Rahmen derselben Kommunikation erfolgt.[5] Nach **Ansicht des BGH sperrt** die Anwendung von § 25 Abs. 1 TDDDG aufgrund der Kollisionsnorm gemäß Art. 95 DSGVO **für diesen Vorgang** die **Anwendung** anderer Regelungen der **DSGVO,** z. B. Art. 6 Abs. 1 lit. f) DSGVO.[6] Es ist nach übereinstimmender Ansicht des EuGH und BGH für das Vorliegen des Einwilligungserfordernisses

[5] EDSA, Guidelines 02/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, Rn. 26 ff.
[6] Vgl. BGH I ZR 7/16 – Cookie-Einwilligung II, Rn. 59.

unbeachtlich, **ob** es sich bei den **Endgeräteinformationen** um **personenbezogene oder anonyme** Daten handelt.[7]

(2) Die **Rechtsprechung** untersagt bislang einhellig unter anderem den **Einsatz** von **Tracking-Anbietern** auf einer Website **ohne Abfrage** einer freiwilligen und informierten **Einwilligung**.[8]

(3) In Rechtsprechung und aufsichtsbehördlichen Positionierungen wurden hinreichend **Anforderungen** an die **Gestaltung** von **Einwilligungsbannern** definiert.[9]

(4) Für die Wirksamkeit der Einwilligung trägt der Website- und App-Betreiber nach Maßgabe der EuGH-Rechtsprechung die **Beweislast**. Denn der EuGH hat jüngst aus Art. 5 Abs. 2 DSGVO nunmehr dem Verantwortlichen ausdrücklich die Darlegungs- und Beweislast für die Rechtsmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO auferlegt.[10]

b) JENTIS Consent Manager

(1) Der **JENTIS Consent Manager verbindet** sich im Browser zu **anderen** installierten **CMPs** wie z.B. OneTrust oder User Centrics, um die Consent Informationen von dort zu erhalten und dann selbst danach die weitere Verarbeitung zu steuern. Der Einsatz des **JENTIS Consent Managers** ermöglicht die Abfrage einer den datenschutzrechtlichen Anforderungen entsprechenden Einwilligung, z. B. für eine Nutzung von Drittanbietertools wie Google Analytics.

Jedoch können Dienste zur Bereitstellung von Nutzerpräferenzen wie der **JENTIS Consent Manager** ohne Abfrage einer Nutzereinwilligung zulässig sein.[11]

(2) Cookies und ähnliche Technologien dürfen auch nach Ansicht der DSK z. B. für etwaige Zusatzfunktionen des Basisdienstes Website genutzt werden, wenn diese vom Nutzer angefordert werden, was beispielsweise beim Einsatz von CMPs der Fall sei.[12] JENTIS DCP verarbeitet die Einwilligung von anderen CMP-Anbietern, , um eine differenzierte Anbindung an andere Drittanbieter-Tools auf Basis der Einwilligungsentscheidung des Nutzers zu ermöglichen. Die Einbindung und Bereitstellung der Funktionen der CMPs durch JENTIS DCP ist in vertretbarer Weise **als in zulässiger Weise einwilligungsfrei** anzusehen.

(3) **JENTIS verarbeitet** bei der Anbindung des JENTIS **Consent Manager** an eine andere installierte CMP **keine** langfristig in den Cookies der CMP gespeicherten **User-IDs**.[13] Da JENTIS keinen Zugriff auf andere CMP-Cookies nehmen kann, die der Kunde in seine Website eingebunden hat, erstellt JENTIS eine eigene Consent-ID serverseitig zur Erfüllung der Protokollierungspflicht der Nutzer-Einwilligung nach Art. 7 Abs. 1 DSGVO und dem Website-Betreiber die Möglichkeit zu geben, etwaiger Auskunftsersuchen von Betroffenen zu erfüllen. Anders als von der DSK in ihrer Orientierungshilfe Telemedien argumentiert,[14] hat JENTIS als externer Dienstanbieter keine Möglichkeit, die Nutzerpräferenzen für die Einstellungen in der CMP in einem Cookie zu speichern, stellt aber sicher, dass bestehende Einwilligungsinformationen in seinen Systemen für

[7] Vgl. EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 70.
[8] Vgl. OLG Köln, Urt. v. 03.11.2023 – 6 U 58/23; LG Frankfurt, Urt. v. 19.10.2021 – 3-06 O 24/21; LG München, Urt. v. 29.11.2022 – 33 O 14776/19.
[9] Vgl. EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 72; DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, S. 35 ff.
[10] EuGH, Urt. v. 04.05.2023 – C-60/22, Rn. 53 ff.; vgl. zur Einwilligung zuletzt EuGH, Urt. v. 04.07.2023 – C-252/21, Rn. 95, 152.
[11] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 7 f.; ICO, Guidance on the use of cookies and similar technologies, S. 37.
[12] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 21.
[13] Vgl. dazu DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26.
[14] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26.

die nachgelagerte Verarbeitungen richtig dargestellt werden. Deshalb lässt sich die Verarbeitung der Consent-ID als „unbedingt erforderlich" nach Art. 5 Abs. 3 S. 2, Var. 2 ePrivacy-RL bzw. § 25 Abs. 2 Nr. 2 TDDDG einordnen (vgl. dazu Pkt. I. 3.a.bb.).

3. Datenerfassung von Non-Consented-Nutzern

JENTIS bietet mit dem JENTIS Essential Mode **(b.)** eine Möglichkeit, bei nicht gegebener Einwilligung Nutzer-Daten auf ein Mindestmaß zu reduzieren, sodass in Abhängigkeit der Risikoaffinität von Unternehmen Ausnahmen vom Einwilligungserfordernis belastet werden können **(a.)**.

a) Ausnahmen von Einwilligungserfordernis für Endgerätezugriff

Von der Pflicht zur Abfrage einer Einwilligung für den Zugriff auf und der Speicherung von Informationen aus Endgeräten der Nutzer beim Online-Tracking existieren in Art. 5 Abs. 3 S. 2 ePrivacy-RL zwei Ausnahmen, die auch in § 25 Abs. 2 TDDDG unverändert übernommen worden sind.

aa) Erforderlichkeit für Durchführung und Erleichterung elektronischer Kommunikation

(1) Für die technisch zwingend veranlasste Übermittlung der IP-Adresse des Nutzers und weiterer Endgeräteinformationen wie z. B. Browser- und Geräteinformationen bei HTTP-basierten Anwendungen ist grundsätzlich der Ausnahmetatbestand in § 25 Abs. 2 Nr. 1 TDDDG einschlägig.

(2) Danach bedarf es **keiner Einwilligung**, wenn eine **technische Speicherung** oder ein Zugriff auf Endgeräteinformationen zur **Durchführung** der **elektronischen Kommunikation** erfolgt. Voraussetzung ist jedoch, dass die Durchführung oder Erleichterung der elektronischen Kommunikation **alleiniger Zweck** der Verarbeitung ist.[15] Der Ausnahmetatbestand in Art. 5 Abs. 3 S. 2 ePrivacy-RL/ § 25 Abs. 2 Nr. 1 TDDDG umfasst nach Ansicht des europäischen Datenschutzgremiums sowie einzelnen Aufsichtsbehörden[16]:

- die Fähigkeit, die Informationen über das Netzwerk zu leiten, insbesondere durch Identifizierung der Kommunikationsendpunkte,
- die Fähigkeit, Datenelemente in ihrer vorgesehenen Reihenfolge auszutauschen, insbesondere durch Nummerierung der Datenpakete sowie
- die Fähigkeit, Übertragungsfehler oder Datenverlust zu erkennen.

bb) Unbedingte Erforderlichkeit zur Bereitstellung eines gewünschten Dienstes

(1) Die **zweite Ausnahme** in Art. 5 Abs. 3 S. 2 ePrivacy-RL, wonach der **Zugriff** auf Endgeräteinformationen **unbedingt erforderlich ist,** um einen vom Nutzer gewünschten Dienst der Informationsgesellschaft **bereitzustellen**, ist nach dem Urteil des BGH jedenfalls nicht für Zwecke der Werbung und Marktforschung einschlägig (I ZR 7/16 – Cookie-Einwilligung II).

(2) Nach **Ansicht** der **DSK** gilt für die **Auslegung** des Begriffes **„unbedingt erforderlich"** mit Blick auf ErwGr. 66 ePrivacy-RL ein **restriktives** (enges) **Verständnis**. Für die unbedingte Erforderlichkeit könne

[15] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 3 f.
[16] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012, S. 3 f.

deshalb **nicht** auf **wirtschaftliche Erwägungen** für die Realisierung eines Geschäftsmodells abgestellt werden.[17]

(3) **Strengere Anforderungen** stellt die DSK an die Belastbarkeit der Ausnahmeregelung für die **Verwendung** von **Cookie-IDs** (Nutzer-IDs). Für derartige Speicherungen bestehe nur in **wenigen Fällen** eine unbedingte Erforderlichkeit, da viele Funktionen, die eine Speicherung oder einen Zugriff auf Endgeräteinformationen bedingen, **ohne** eine **Individualisierung erfolgen** können. Als **Negativbeispiel** führt die DSK z. B. die Nutzung einer **langfristig gespeicherten ID** für folgende Use Cases an:

- Protokollierung einer Einwilligung in einer Consent-Management-Plattform (CMP),
- Load-Balancing sowie
- Speichern von Einstellungen zur Sprache oder der Hintergrundfarbe.

(4) Nach Ansicht der Datenschutzkonferenz sind maßgebende **Kriterien** für die Bestimmung der **unbedingten Erforderlichkeit**[18]:

- **Zeitpunkt** der Speicherung – Wann darf der Auslese- und Speichervorgang stattfinden?
- **Inhalt** der Informationen – Welche Informationen werden gespeichert und ausgelesen?
- **Dauer** der Speicherung der Informationen – Wie lange werden Informationen auf den Endgeräten gespeichert und für welchen Zeitraum können sie ausgelesen werden?
    - Der Zeitraum der Speicherung dürfe nur so lang gewählt werden, wie für die Umsetzung der granularen Funktion des Telemediendienstes erforderlich sei.
    - Grundsätzlich seien Session-Cookies eher erforderlich als langlebige Cookies.
- **Auslesbarkeit** der Informationen – Für wen sind Informationen vom Endgerät auslesbar und verwertbar?
    - Werden Informationen auf dem Endgerät der Nutzer bei der Inanspruchnahme eines Telemediums gespeichert, müsse technisch sichergestellt werden, dass diese nachfolgend grundsätzlich nur von den Betreibern der jeweiligen Website ausgelesen werden könnten. Maßgebend hierfür ist u. a. die Domäne eines Cookies, die darüber entscheidet, wer die Information auslesen kann.
    - Bei Third-Party-Diensten sei dies gerade nicht der Fall, so dass sichergestellt sein müsse, dass Drittdienstleister die ausgelesenen Informationen grundsätzlich ausschließlich für die von Nutzern aufgerufene Website verwenden.

(5) Im Rahmen einer **Erforderlichkeitsprüfung,** bezogen auf **das Third-Party-Tracking** z. B. für Nutzeranalysen, wird man mit hinreichender Sicherheit zu dem Ergebnis gelangen, dass ohne Modifikation der Tracking-Parameter **keine unbedingte Erforderlichkeit** nach § 25 Abs. 2 TDDDG vorliegen kann, da ein Third-Party-Tracking stets den Kreis der Datenempfänger über den eigentlichen Diensteanbieter hinaus erweitert.

Solange ein vom Website- und App-Betreiber selbst vorgenommenes Tracking mit gleicher Eignung ohne Einsatz von Drittanbietern möglich ist, wird man unter Berücksichtigung der genannten

[17] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, Rn. 76; Österreichischer VGH, Urt. v. 31.10.2023 – Rn. 2020/04/0024.
[18] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, Rn. 93 f.

EuGH-Rechtsprechung und der Auffassung der DSK zum Online-Tracking nicht zur Erforderlichkeit des Einsatzes von Drittanbietern gelangen.[19]

b) JENTIS Essential Mode als Fall-Back-Lösung

(1) Vorbehaltlich einer künftig anderslautenden Positionierung von Aufsichtsbehörden oder der Rechtsprechung, JENTIS ermöglicht es Website-Betreibern, das Website-Tracking so zu konfigurieren, dass die Ausnahmevorschrift vom Einwilligungserfordernis in Art. 5 Abs. 3 S. 2 ePrivacy-RL bzw. § 25 Abs. 2 Nr. 2 TDDDG rechtskonform angewendet wird.

Durch die Verwendung von First-Party-Daten und die **Minimierung** der **Datenparameter auf** das technisch Notwendige bzw. das **unbedingt Erforderliche** kann der Kunde die Nutzerdaten über das Feature **Essential Mode als Fall-Back-Lösung** verfolgen, wenn der Nutzer seine Zustimmung nicht erteilt.

Die Belastbarkeit der Ausnahmeregelung nach § 25 Abs. 2 Nr. 2 TDDDG für den notwendigen Zugriff auf das Endgerät in Form eines First-Party-Cookies setzt dabei voraus, dass der „Essential Mode“[20] innerhalb der **JENTIS DCP** aktiviert und in einer bestimmten Weise durch den Kunden selbstständig wird. Nachstehend ist ein Beispiel für die Konfigurierung des Essential Mode-Features zu finden (siehe Punkt (4) aa). Durch Aktivierung des Features Essential Mode wird lediglich das Dashboard im User Interface des Accounts angepasst. Der Website-Betreiber hat die volle Kontrolle über die Systemeinstellungen und -konfigurationen und muss Konfiguration der JENTIS Server Suite selbstständig vornehmen.

Im Ausgangspunkt steht der Anwendung der Ausnahmevorschriften nicht entgegen, dass das First-Party-Cookie von JENTIS **multifunktional** eingesetzt wird, weil es für mehrere **unterschiedliche Zwecke** verwendet wird.[21]

(2) Die aufgrund der Serveranfrage des Browsers des Nutzers an den JENTIS Server erfolgte **Auslieferung** des **First-Party-Cookies von JENTIS** bedingt einen Zugriff auf Endgerätekapazitäten des Browsers des Nutzers.

Die in der **Serverantwort** des JENTIS-Servers erfolgte **Speicherung** eines **First-Party-Cookies** nebst zufällig generierter **Client-ID dient** der Wiedererkennung des Endgeräts als **JENTIS Tracker** (vgl. Pkt. I.1.b.), um mithilfe eines serverseitigen Taggings eine **reduzierende** und **substituierende Filterung** von **Datenströmen** zu ermöglichen, bevor diese an Drittanbieter wie Google oder Adobe weitergeleitet werden. Dadurch wird der Verlust der Kontrolle beim Einsatz von Tracking-Anwendungen von vornherein verhindert und eine **rechtmäßige Datenverarbeitung** ermöglicht.

(3) Die durch die JENTIS Twin-Server-Technologie ermöglichte **Reduzierung** und **Modifizierung** der **Datenparameter** für das Server Side Tracking, die im Zuge der Nutzerkommunikation mit der Website abgefragt werden, **lässt sich** im Einklang mit der Auffassung des Europäischen Datenschutzbeauftragten („**EDPS**“) in vertretbarer Weise **auf** die **Ausnahme vom Einwilligungserfordernis** gemäß Art. 5 Abs. 3 S. 2 Var. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TDDDG **stützen**.

Der **EDPS** hat ein „**Toolkit**“ zur **Festlegung** für die **Beurteilung** der **„Erforderlichkeit“** von Maßnahmen in Übereinstimmung mit Art. 52 Abs. 1 GRCh veröffentlicht.[22]

---

[19] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 27.
[20] Essential Mode.
[21] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 24.
[22] EDPS, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, 2017, S. 5.

Diese **Kriterien** können nach Medieninformationen auch der Ansicht der Datenschutzorganisation „La Quadrature du Net“ zufolge als **Orientierung** für die **Auslegung** des **Begriffs** der „**Erforderlichkeit**“ nach der Art. 5 Abs. 3 S. 2 ePrivacy-RL **dienen**. Ebenso hat der **EDPB** in den „Leitlinien 2/2019“[23] zur Auslegung des Begriffs der Erforderlichkeit **auf** das **Toolkit** des **EDPS** für den nicht-öffentlichen Bereich **Bezug genommen**.[24] Deshalb wird auch in der **Fachliteratur** zutreffend vertreten, dass die Checkliste für die Bestimmung der „unbedingten Erforderlichkeit“ in Art. 5 Abs. 3 S. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TDDDG verwendet werden kann.[25]

Vorbehaltlich künftiger Rechtsprechung und aufsichtsbehördlicher Positionierungen kann die **Methodik** eine Grundlage für die Aktivierung ausgewählter Funktionalitäten auf Websites bilden und der unter Pkt. B. **geschilderten Rechtsunsicherheit entgegenwirken**.

(4) Laut EDPS impliziert die **Erforderlichkeit** das Erfordernis einer kombinierten, auf Fakten gestützten Bewertung der Wirksamkeit der Maßnahme mit Blick auf das angestrebte Ziel und auf die Frage, ob sie im Vergleich zu anderen Optionen für das Erreichen desselben Ziels weniger eingreifend ist. Die **Checkliste für die Beurteilung der Erforderlichkeit** besteht aus **vier** aufeinander folgenden **Schritten**. Jeder Schritt entspricht einer Reihe von Fragen, die die Beurteilung der Erforderlichkeit erleichtern.[26]

aa) Beispielkonfiguration für Essential Mode

Nachfolgend wird eine **beispielhafte Konfiguration** für den **Essential Mode** von **JENTIS** vorgeschlagen, die nach unserem Dafürhalten aufgrund der Anwendung des EDPS Necessity Toolkit zur Auslegung der Erforderlichkeit den Einsatz der Tracking-Proxy-Technologie in vertretbarer Weise als „**unbedingt erforderlich**“ ohne Vorliegen einer Nutzereinwilligung bei Akzeptanz von Restrisiken rechtfertigen lässt.

- **Schritt 1 EDPS Necessity Toolkit:** Die für das EDPS-Toolkit zur Bestimmung der Erforderlichkeit des Endgerätezugriffs verlangte detaillierte faktische Darstellung des technischen Funktionsprinzips zur Bereinigung der Tracking-Daten von Drittanbieter-Diensten wie Google Analytics und Reduzierung der Nutzerdaten sowie Zweckfestlegung ist erfolgt.
- **Schritt 2 EDPS Necessity Toolkit**: Die für Schritt 2 des EDPS-Toolkits erforderliche Beantwortung von Fragen zur Bestimmung der Tragweite der Eingriffsintensität der JENTIS DCP ist in Anbetracht der detaillierten Beschreibung der einzelnen Datenverarbeitungsschritte ebenfalls erfolgt.
- **Schritt 3 EDPS Necessity Toolkit:** Als Schritt 3 des EDPS-Toolkits wurde als Use Case das Ziel einer grundlegenden statistischen Analyse des Nutzungsverhaltens auf der Website, einer reduzierten Messung von Conversions identifiziert, um in Ausprägung der von Art. 16 Abs. 1 EU-Grundrechte-Charta gewährleisteten unternehmerischen Freiheit digitale Angebote zu optimieren, verbessern und dem Stand der Technik entsprechend weiterzuentwickeln. Art. 23 DSGVO enthält nach Ansicht des EDPS eine Auflistung von Zielen, aufgrund derer legitimerweise die Rechte natürlicher Personen und die Pflichten des Verantwortlichen eingeschränkt werden können. Hierzu zählt nach Art.

[23] EDPB, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, V2.0.
[24] EDPB, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, V2.0, S. 9, Fn. 19.
[25] Hense, in: Taeger/Pohle, Computerrechts-Handbuch, 2022, 37. EL, Projektspezifischer Datenschutz, Rn. 112.
[26] EDPS, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, 2017, S. 10.

23 Abs. 1 lit. i) DSGVO auch der Schutz der Rechte und Freiheiten anderer Personen, sprich auch juristischer Personen und deren nach Art. 16 Abs. 1 GRCh zu berücksichtigenden unternehmerischen Freiheiten.

- **Schritt 4 EDPS Necessity Toolkit:** JENTIS SaaS stellt sicher, dass spezifische Aspekte für die Prüfung der Erforderlichkeit gemäß Schritt 4 des EDSB-Toolkits durch das Essential Mode abgedeckt werden können. In die **nachfolgende Beispielkonfiguration** des **Essential Mode** von **JENTIS** wurde Folgendes berücksichtigt:
  - **Modifizierung der Client-ID von Drittanbieterdiensten wie Google Analytics:**
    - Die Client-ID/User-ID von Drittanbieterdiensten wie Google Analytics, die eine eindeutige Zuordnung des Endgerätes ermöglicht, muss vollständig synthetisiert, d.h. durch eine fiktive, zufällig generierte Client-ID/User-ID ersetzt werden.
    - Die JENTIS User-ID wird als First-Party-Cookie über die Domäne des Kunden im Browser des Nutzers gespeichert. Die Verarbeitung der selbst von JENTIS vergebenen User-ID stellt die einzige Referenz für die Wiedererkennung des Browsers des Nutzers dar.
    - Nach Ansicht des BGH stellt eine in Cookies gespeicherte zufallsgenerierten Nummer (**Cookie ID**), die als **Endgeräteinformation** Registrierungsdaten des Nutzers zugeordnet ist, ein **Pseudonym** i. S. d. § 15 Abs. 3 TMG dar, wobei der BGH noch auf die Legaldefinition in § 3 Abs. 6a BDSG a.F. abstellte.[27]
    - Die Speicherdauer der JENTIS Cookies in das Essential Mode sollte auf maximal 13 Monate eingestellt werden.
    - Die nach Art. 4 Nr. 5 DSGVO erforderliche Einschränkung, dass die Zusatzinformationen separiert aufbewahrt werden und durch technisch-organisatorische Maßnahmen abgesichert sind, die absichern, dass keine Zuweisung der Daten zu einer identifizierbaren Person erfolgt, wird umgesetzt. Unabhängig davon, ob die zusätzliche Information eine direkte Zuordnung oder eine Zuordnungsregel sein kann,[28] wird die technische und organisatorische Absicherung mittels einer **robusten Trennung** der System-Cluster **Serverinstanzen** im Rahmen eines **Server-Side-Tracking** von JENTIS sichergestellt.
    - Die Verarbeitung durch die JENTIS Server erfolgt auf getrennten Dateninstanzen, auf dem ggf. Bestandsdaten von Nutzern (z. B. E-Commerce-Shop) gespeichert werden.
  - **Kürzung der IP-Adresse:**
    - Die IP-Adresse des Nutzers wird auf Server von JENTIS um das letzte Oktett gekürzt; es findet keine Kommunikation des Browsers des Nutzers mit Google Servern statt. Im Fall einer **Teil-Unkenntlichmachung** der IP-Adressen durch Kürzung des letzten Oktetts nach Übermittlung der vollständigen IP-Adresse ist nach Ansicht der Rechtsprechung von einer **Pseudonymisierung** i. S. d. § 3 Abs. 6a BDSG a.F. auszugehen, wie eine rechtskräftige Entscheidung des LG Frankfurt zum Webanalysedienst „Piwik“ zeigt.[29]

[27] BGH, Urt. v. 28.05.2020 – I ZR 7/16 – Cookie Einwilligung II, Rn. 72; zustimmend in Bezug auf die DSGVO Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[28] Schwartmann/Weiß, Entwurf für einen Code of Conduct zum Einsatz DSGVO konformer Pseudonymisierung, 2019, v1.0, S. 11.
[29] LG Frankfurt, Urt. v. 18.2.2014 – 3-10 O 86/12, Rn. 36; zustimmend Weidert/Klar, BB 2017, 1858, 1859.

- Dabei lehnte das Gericht die Einordnung der Kürzung der IP-Adresse als Mittel der Anonymisierung insbesondere deswegen ab, weil ein Website-Betreiber, der über Registrierungsdaten aus Nutzerkonten verfügt, jederzeit in Echtzeit eine Zuordnung zu Identifikationsmerkmalen vornehmen könnte.

- **Entfernung von Click-IDs in URLs:**
  - Sollte der Nutzer eine Kunden-Website über die Suchmaschine google.com aufrufen, sollte die Google Click ID als URL-Parameter („gclid“)[30] entfernt werden.
- **Modifizierung von kundenspezifischen IDs:**
  - Ebenso werden Datenparameter, die eine eindeutige Identifizierung der Nutzer ermöglichen, z. B. Order-IDs oder Lead-IDs von JENTIS nicht verarbeitet, sondern als Zufallsprodukt neu erzeugt.
  - Dabei wird eine zufällige UUID (Universally Unique Identifier, eine 128-Bit-Zahl) erzeugt.
- **Modifizierung des User Agent:**
  - Der User Agent wird gelöscht und durch einen neuerzeugten User Agent ersetzt.
- **Kein Fingerprinting:**
  - Es darf keine Kombination von Browser- und Geräteeinstellungen zur Identifizierung und Wiedererkennung von Nutzern erfolgen.
- **Zweckreduktion:**
  - Die Zwecke im Rahmen des Use Case „Analyse“ wurden darauf beschränkt, die Bewertung veröffentlichter Inhalte und der Nutzerfreundlichkeit der Webseite zu ermöglichen und die Wirksamkeit gestalterischen Entscheidung der Website zu bewerten oder zu verbessern.
  - Der Einsatz der Analyse sollte aus Kundensicht auf die Erstellung anonymer Statistiken beschränkt werden.
- **Keine Zusammenführung von IDs:**
  - Die JENTIS User-ID wird nicht mit anderen Nutzerdaten wie einer CRM-ID oder Systemen mit Registrierungsdaten zusammengeführt.
- **Unschärfegrade bei Timestamps:**
  - Sofern eine Re-Identifizierung eines Nutzers oder ein singling-out eines einzelnen Nutzers anhand des Timestamps einer Browser-Session möglich ist, können mithilfe der JENTIS-Twin-Server-Technologie die Zeitangaben durch synthetisierte Werte (fiktive Zeitstempel) ersetzt werden.
  - Alternativ kann mithilfe der JENTIS-Twin-Server-Technologie bei einem gleichzeitigen Mindestaufkommen im jeweils gemessenen Zeitabschnitt in einer homogenen Gruppe eine bloße Mindestunschärfe der Timestamps ausreichend sein. Von dem Erreichen eines homogenen Mindestaufkommens von Nutzern, sprich einer Gruppe von Nutzern,

[30] Prüfung der automatischen Tag-Kennzeichnung von Google Ads.

die dieselben Attribute teilen, hängt der Unschärfegrad der Timestamps (Cluster auf Stunden- oder Minutenbasis) im Einzelfall ab.

bb) Anforderungen der Aufsichtsbehörden

(1) Ergänzend zum EDPB-Toolkit führt auch unter **Anwendung** der **Auslegungskriterien** der **DSK** für die „unbedingte Erforderlichkeit" (vgl. Pkt. I.3.a.bb.) und der **CNIL** für den Einsatz von Tracking-Proxys zu **keinem anderen Ergebnis**.

(2) Die **strengen Anforderungen** der **DSK** an die Belastbarkeit der Ausnahmeregelung für die **Verwendung** von in Cookies gespeicherten **Nutzer-IDs** (Cookie-IDs) werden bei Zugrundelegung des Funktionsprinzips des Essential Mode von JENTIS erfüllt:

- Zunächst schließt die DSK die Belastbarkeit der Ausnahmeregelung in Art 5 Abs. 3 S. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TDDDG für die Reichweitenmessung und/oder Analyse von Website-Besucherzahlen per-se nicht aus.[31]
- Der Zeitpunkt der Speicherung des Session-Cookies und das Auslesen der Client-ID findet im Zuge der Auslieferung der Website nach Interaktion mit dem Cookie-Banner statt.
- Nach Maßgabe der vorstehenden Beispielkonfiguration des Essential Mode für Google Analytics werden sämtliche Identifikatoren mit Ausnahme der JENTIS-User-ID reduziert und synthetisiert**.** Der First-Party-Cooke wird über die Domäne des Kunden im Browser des Nutzers gespeichert.
- Die Speicherdauer der First-Party-Cookies kann individuell je nach Risikoaffinität entweder wenige Minuten – einzelnen Besuche (Sitzungen) sind dann nicht mehr zusammenführbar – oder bis zu 13 Monate festgelegt werden. Nach Lesart der Orientierungshilfe der DSK stellt das Kriterium der Speicherdauer lediglich eines von mehreren Kriterien dar und ist allein nicht ausschlaggebend für die rechtliche Beurteilung der „unbedingten Erforderlichkeit".[32]
- Der Endgerätezugriff erfolgt ausschließlich durch die Server von JENTIS als Auftragsverarbeiter. Es erfolgt kein clientseitiger Endgerätezugriff durch Server von Google oder anderer Drittanbieter.
- Insbesondere wird bei entsprechender Konfiguration von JENTIS auch der Anforderung aus Art. 5 Abs. 3 S. 2 ePrivacy-RL bzw. § 25 Abs. 2 Nr. 2 TDDDG „vom Nutzer ausdrücklich gewünschten Telemediendienst" entsprochen. Denn im Einklang mit der Ansicht der DSK wird in erster Linie den Interessen der Nutzer der Website Rechnung getragen. Dabei bleiben die Interessen der Drittanbieter aufgrund der Modifizierung von Datenparametern außer Betracht. Die Interessen der Betroffen wird durch folgende Gesichtspunkte gestärkt:
    - Verhinderung unmittelbarer Zugriffe von Drittanbietern auf Endgerät von Nutzer:innen;
    - Zugriffsbeschränkungen und Kontrolle über die Weitergabe der Daten an Drittanbieter
    - Privacy Enhancement durch Minimierung der Nutzerdatenparameter, um eine Wiedererkennung zu verhindern und
    - Sicherstellung der Rechtskonformität.

[31] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 22.
[32] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26 f.

(3) Schließlich können ebenso die **Anforderungen** der französischen Aufsichtsbehörde („**CNIL**“) an Proxy-Lösungen[33] beim Einsatz von Tracking-Diensten mit Hilfe der technischen Möglichkeiten von JENTIS erfüllt werden, die, soweit ersichtlich, als erste europäische Behörde den Einsatz von Proxy-Lösungen für den Einsatz von Google Analytics empfiehlt. Das BayLDA hat sich dieser Rechtsauffassung angeschlossen.[34]

- keine Übermittlung der vollständigen IP-Adresse des Nutzers an Server von Tracking-Diensten.
- Die Client-IDs und Nutzer-IDs, die von Drittanbietern vergeben werden, werden durch den JENTIS-Server vollständig ersetzt.
- Die Browser- und Geräte-Informationen lassen nach Maßgabe der Beispielkonfiguration des Essential Modes für Google Analytics aufgrund der gebildeten künstlichen Werte, insbesondere für den User Agent, keine Identifizierung durch die Drittanbieter zu. Auf diesem Wege kann ein Fingerprinting verhindert werden. Der Algorithmus, der die Ersetzung der Browser-Informationen vornimmt, gewährleistet ein ausreichendes Maß an Kollisionen (d. h. eine ausreichende Wahrscheinlichkeit, dass zwei verschiedene Kennungen nach der Modifizierung ein identisches Ergebnis liefern).
- Referrer können gelöscht werden (Hinweis: bei Entfernung des Referer leidet die Qualität der Analyse).
- Etwaige in den gesammelten URLs enthaltene Tracking-Parameter können individuell gelöscht oder ersetzt werden (z. B. die „UTM-Parameter“, aber auch die URL-Parameter, die das interne Routing der Website ermöglichen).
- Die vom Tracking Proxy vergebene Client-ID zur Wiedererkennung des Browser-Nutzers oder deterministisch mitgeteilte IDs (CRM, eindeutige ID) lassen keine websiteübergreifende (Cross-Site) oder geräteübergreifende Erfassung (Cross-Device) des Nutzerverhaltens zu.
- Sämtliche Nutzerdaten, die eine Re-Identifizierung durch Tracking-Anbieter ermöglichen können, werden gelöscht.

cc) Anwendung der Behördenanforderungen auf Essential Mode

(1) Zusammenfassend lässt sich festhalten, dass der JENTIS Essential Mode Website-Betreibern ermöglicht, sich auf die Ausnahmeregelung vom Einwilligungserfordernis gemäß Art. 5 Abs. 3 S. 2 Var. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TDDDG aufgrund der folgenden Aspekte berufen können:

- Verhinderung unmittelbarer Zugriffe von Drittanbietern auf Endgerät von Nutzer
- Vollständige Kontrolle über einzelne Datenpunkte
- Reduzierung oder Modifizierung von Datenpunkten
- Zugriffsbeschränkungen und Kontrolle über die Weitergabe der Daten an Drittanbieter
- Festlegung von Bedingungen für Datenweitergabe
- Förderung (Enabler) der Verbesserung der Privatsphäre der Nutzer
- Sicherstellung der Rechtskonformität.

(2) Die entsprechende Anwendung der JENTIS-Twin-Server-Technologie führt zu einer weiteren Erschwerung der Zuordnung eines Browsers eines Endgerätes zu einem Nutzungsprofil als einzige Referenz für die spätere Wiedererkennung des Browsers und stellt daher als Privacy-Enhancing-Technologie eine **wirksame**

[33] CNIL, Mesure d'audience et transferts de données.
[34] BayLDA, 12. Jahresbericht 2022, S. 50 ff.

Maßnahme dar, die im Rahmen eines First-Party-Endgerätezugriffs, den geringsten Eingriff in die Grundrechte aus Art. 7 und Art. 8 Abs. 1 EU-Grundrechte-Charta der Website-Besucher bedeutet.

(3) In der Gretchenfrage, was denn nun „unbedingt erforderlich" in den Ausnahmeregelungen zum strikten Einwilligungserfordernis nach Art. 5 Abs. 3 ePrivacy-RL bedeuten soll, werden Gerichte und nicht der Gesetzgeber das letzte Wort haben. In den neuen EDSA „Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive" sucht man entsprechende Auslegungskriterien noch vergebens, der Österreichische VGH[35] hat hingegen der von Medienunternehmen postulierten „wirtschaftlichen" Interpretation von „unbedingter Erforderlichkeit" eine klare Absage erteilt.

Ebenso wenig kann es auf eine wie auch immer festzustellende „technische Notwendigkeit" ankommen, denn Erwägungsgrund 24 ePrivacy-RL spricht eine eindeutige Sprache, wenn es um den Grundsatz der Technologieneutralität geht. „Unbedingt erforderlich" ist entlang des Telos der Norm auszulegen, dem Schutz der Privatsphäre. Nur eine Auslegung, deren Blick sich auf das Verarbeitungsergebnis richtet, kann den Einsatz von Privatsphäre schützenden Privacy Enhancing Technologien rechtfertigen. Ein Endgerätezugriff, der dem Schutz der Privatsphäre zu dienen bestimmt ist, wird man demnach als zulässig erachten können.

(4) Sofern eine Berufung auf die Ausnahmevorschrift in Art. 5 Abs. 3 S. 2 Privacy-RL bzw. § 25 Abs. 2 TDDDG möglich ist, bedarf es zwar keiner Einwilligung der Nutzer. Dennoch ist zwingend zu prüfen, ob für den jeweiligen Dienst die **Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO** einschlägig ist. Für die notwendige **Dokumentation** der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO[36] sollte **ein sog. LIA (Legitimate Interests Assessment)** nach Maßgabe der vom Kunde vorgenommenen Konfiguration der JENTIS DCP durchgeführt werden, um einen Nachweis für die erfolgte Interessenabwägung im Einzelfall erbringen zu können und die **Compliance** in der Supply Chain sicherzustellen. JENTIS stellt den Kunden für eine beispielhafte Konfiguration des Essential Modes ein Legitimate Interests Assessment zur Verfügung.

4. Weitergabe substituierter Daten an Drittanbieter-Systeme über JENTIS Tool Connector

(1) **Nachgelagerte Verarbeitungen**, d. h. die sich an den gerechtfertigten Endgerätezugriff anschließende Verarbeitung wie die Analyse der Web- und App-Nutzung in eigenen und fremden Systemen, unterliegen nicht dem **Anwendungsbereich** des TDDDG, sondern der **DSGVO**.[37] Für nachgelagerte Verarbeitungen ist daher auf die Rechtsgrundlagen aus Art. 6 Abs. 1 DSGVO abzustellen.[38]

(2) Als weitere Verarbeitungsvorgänge, die sich an den Endgerätezugriff durch JENTIS-Server anschließen, sind die serverseitigen Übermittlungen der bereinigten Tracking-Daten Server von Drittanbieter wie Google zu bewerten.

Die JENTIS DCP lässt sich so konfigurieren, dass weder eine Übertragung der von Drittanbietern wie Google vergebenen Client-ID noch der IP-Adresse des Nutzers erfolgt. Bei der Kommunikation des JENTIS-Servers von Drittanbietern wie Google würden dann ausschließlich die bereinigten Tracking-Daten – die neu erzeugte Client-ID, die IP-Adresse des Website-Servers, der synthetisierte User Agent und die synthetisierte Order-ID übermittelt werden.

---

[35] Österreichischer VGH, Urteil v. 31.10.2023, Gz. Ro 2020/04/0024.
[36] EDPB, WP 260, Anhang.
[37] Vgl. EuGH Urt. v. 15.06.2021 – C-645/19 – One-Stop-Shop, Rn. 74; BT-Drs. 19/27441, S. 38; EDSA, Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO, S. 23.
[38] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, S. 31.

Die nach Modifizierung der Tracking-Parameter erfolgte Übermittlung an Drittanbieter wie Google lässt sich bei Durchführung eines **Legitimate Interests Assessment** für die kundenspezifischen Use Cases auf die Rechtsgrundlage in Art. 6 Abs. 1 S. 1 lit. f) DSGVO stützen.

(3) JENTIS SaaS ermöglicht neben den üblichen Datensubstitutionen, die zu Pseudonymisierungen und Anonymisierungen führen, auch die technische Möglichkeit, Daten zu synthetisieren. Die Bildung von **synthetischen Daten** aus realen Rohdaten **entspricht** der Bildung von Datenwerten **nach dem Zufallsprinzip,** soweit es um die **Einordnung der Modifizierung als** Maßnahme der **Pseudonymisierung** geht.

- Pseudonymisierung stellt ein geeignetes Privacy Pattern im Rahmen von „Privacy by Design" dar[39] und kann bei „JENTIS" auf der Ebene der Verarbeitung und vor der Weitergabe an Drittanbietern angewendet werden. Nach Ansicht des BGH stellt bereits eine in Cookies gespeicherte zufallsgenerierten Nummer (Cookie ID), die als Endgeräteinformation Registrierungsdaten des Nutzers zugeordnet ist, ein Pseudonym i. S. d. § 15 Abs. 3 TMG dar, wobei der BGH noch auf die Legaldefinition in § 3 Abs. 6a BDSG a.F. abstellte.[40] Gleiches muss in der Konsequenz auch für andere Identifier wie Device IDs, IDFA, GAID und Universal IDs gelten.
- Die **ENISA** (European Union Agency for Cybersecurity) beschreibt „**synthetische Daten**" im Kontext des Datenschutzrechts als neuen Bereich der Datenverarbeitung, in dem Daten so aufbereitet werden, dass sie realen Daten (sowohl personenbezogenen als auch nicht-personenbezogenen) realistisch ähneln, sich aber nicht auf eine bestimmte identifizierte oder identifizierbare Person oder auf das „reale Ausmaß eines zu bewertenden Datenparameters" beziehen.[41]
- Laut **EDPS** können „**synthetische Daten**" als Technologie zur Verbesserung des Schutzes der Privatsphäre (**Privacy Enhancing Technology**) betrachtet werden und in diesem Sinne als Maßnahme der Pseudonymisierung eingesetzt werden.[42] Die Synthetisierung dient nach Ansicht der **ENISA** in erster Linie der **Vertraulichkeit** der **Verarbeitung**,[43] die den Charakter „zusätzlicher Maßnahmen" in technischer und organisatorischer Hinsicht i .S. d. Art. 32 DSGVO aufweist.
- Im Fall der Use Cases beim Einsatz der JENTIS DCP, z. B. bei der Website-Analyse, ist die Wiedererkennung des Nutzers über die **JENTIS User-ID** für Website-Betreiber möglich. Soweit mindestens die „Client-ID des Drittanbieters" sowie im Idealfall weitere **Tracking-Parameter** wie User Agent und etwaige kundenspezifische IDs nach entsprechender Konfiguration der JENTIS DCP **synthetisiert** werden, weisen die übermittelten Datensätze aus Sicht des Empfängers keinen Personenbezug auf, weil die Zuordnungsregel über die JENTIS User-ID zu einem Endgerät ausschließlich bei JENTIS und Website-Betreibern liegt. Lediglich JENTIS als Auftragsverarbeiter und der Website-Betreiber, nicht aber Drittanbieter wie Google verfügen über die Zuordnungsregel – z. B. über die JENTIS User-ID – für die pseudonymen Tracking-Parameter. Es ist dann von einer **wirksamen Pseudonymisierung** nach Maßgabe von Art. 4 Nr. 5 DSGVO auszugehen.

[39] Vgl. BGH, Urt. v. 15.5.2018 – VI ZR 233/17 Rn. 26.
[40] BGH, Urt. v. 28.05.2020 – I ZR 7/16 – Cookie Einwilligung II, Rn. 72; zustimmend in Bezug auf DSGVO Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[41] Vgl. ENISA, Data Protection Engineering, 2022, S. 17.
[42] EDPS, techsonar 2021-2022, S. 10.
[43] Vgl. ENISA, Data Protection Engineering, 2022, S. 17.

- Die **Modifizierung realer Rohdaten** wie die von Drittanbietern vergebene Client-ID oder User-ID ist **unter denselben Bedingungen** wie die **Bildung** von **Hashwerten** aus realen Rohdaten als Pseudonymisierung i. S. v. Art. 4 Nr. 5 DSGVO einzuordnen.[44] Solange die an der Stelle von Client-IDs und User-IDs verwendeten **künstlichen Werte irreversibel** sind, die **Kollisionsfreiheit** der aufbereiteten Datenparameter **sichergestellt** ist **und** die **IP-Adresse** des Nutzers **ersetzt** wurde, ist unter Berücksichtigung der einhelligen Beurteilung zu Hashwerten mangels entgegenstehender Stellunghamen oder Rechtsprechung von einer **DSGVO-konformen Pseudonymisierung** auszugehen.

(4) Die nach Art. 4 Nr. 5 DSGVO **erforderliche Einschränkung**, dass die **Zusatzinformationen separiert aufbewahrt** werden und durch technisch-organisatorische Maßnahmen abgesichert sind, die sicherstellen, dass keine Zuweisung der Daten zu einer identifizierbaren Person erfolgt, **wird** während der Kommunikation der unterschiedlichen Serverinstanzen **von JENTIS umgesetzt**. Unabhängig davon, ob die zusätzliche Information wie die JENTIS User-ID eine direkte Zuordnung oder eine Zuordnungsregel für die neu erzeugten Client-IDs und Order-IDs der Drittanbieter sein kann,[45] ist laut der Produktbeschreibung angesichts der Systemarchitektur von JENTIS eine robuste Trennung der Dateninstanzen gegeben, die eine Zuordnung für Drittanbieter ausschließt.

(5) Soweit ersichtlich, erhalten Drittanbieter wie Google bei den skizzierten Datenübermittlungen im Nachgang des Endgerätezugriffs lediglich eine von JENTIS **neu erzeugte Client-ID**, die nicht mit der von Google vergebenen Client-ID oder User-ID für Google Analytics übereinstimmt und deswegen **keine Zuordnung** der mitgelieferten Informationen **über das Nutzungsverhalten** von Website-Besuchern durch Google ermöglicht.

(6) Ebenso ist **kein Zugriff auf** die **JENTIS DCP** durch **Drittanbieter** wie Google auf Grundlage der zur Verfügung gestellten technischen Dokumentationen möglich. Es erfolgt **keine** direkte **Kommunikation** des **Browsers** des Nutzers **mit Drittanbietern**. Soweit ersichtlich, existiert zu der Frage, ob weiterhin von einem Personenbezug auszugehen ist, wenn lediglich ein Dritter über die Zuordnungsregel für die übermittelten pseudonymen Datensätze verfügt, jedoch keine rechtliche Möglichkeit für den Zugriff auf Identifizierungsmerkmale vorhanden ist, keine anderslautende als die Rechtsprechung des EuGH zum Personenbezug von IP-Adressen.[46]

(7) Im Einklang mit der Ansicht des EuGH[47] ist die Übermittlung der bereinigten Tracking-Daten als nachgelagerte Verarbeitungsphase einzuordnen, die dem Anwendungsbereich der DSGVO unterliegt. Aufgrund der ergriffenen Schutzmaßnahmen – Entfernung der IP-Adresse, Zuordnung von neu erzeugten Werten für die Client-ID und Order-ID, für die Google keine Zuordnungsregel besitzt – lässt sich für die Übermittlung vorbehaltlich einer künftig anderslautenden Rechtsprechung die **Rechtsgrundlage** gemäß **Art. 6 Abs. 1 S. 1 lit. f) DSGVO** in vertretbarer Weise anwenden.

Dabei ist jedoch zwingend zu prüfen, ob die **Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO** einschlägig ist. Für die notwendige **Dokumentation** der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f)

---

[44] Vgl. zum Hashing als valide Maßnahme zur Pseudonymisierung Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 26; ENISA, Pseudonymisation techniques and best practices, 2019, S. 33; ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, S. 12; Artikel 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, S. 20.
[45] Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 11 f.
[46] Vgl. auch Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Rn. 12.
[47] EuGH, Urt. v. 15.06.2021 – C-645/19 – One-Stop-Shop, Rn. 74.

DSGVO[48] sollte **ein sog. LIA (Legitimate Interests Assessment)** durchgeführt werden, um einen Nachweis für die erfolgte Interessenabwägung erbringen zu können. JENTIS stellt den Kunden für eine beispielhafte Konfiguration des Essential Modes ein Legitimate Interests Assessment zur Verfügung.

II. Wie JENTIS DCP hilft, rechtliche Risiken auszuräumen

1. DSGVO-Compliance durch Privacy by Design und Privacy by Default

(1) **Privacy by Design** als **Konzept** wurde im Zuge der Vorstellung eines wissenschaftlichen Beitrags zu „Privacy Enhancing Technologies" (PET) von John Borking 1995 eingeführt,[49] von Ann Cavoukian bis 2010 zu einem systemischen Ansatz[50] entwickelt und ist **international anerkannt**.

(2) Bei der Produktentwicklung der JENTIS DCP wurden entsprechend den EDPB-Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[51] **(a.)** die Bausteine für die Umsetzung des Konzepts von Privacy by Design implementiert **(b.)** und ermöglichen einen DSGVO-konformen Einsatz von Online-Marketing-Tools.

(3) JENTIS DCP als SaaS-Produkt berücksichtigt „Privacy by Design"-Strategien als Leitlinien, um sicherzustellen, dass die Umsetzung des Konzepts „Privacy by Design" und „Privacy by Default" durch die Website-Betreiber (seine Kunden) verfügbar und möglich ist. Hierzu wurden datenorientierte Strategien wie „minimieren", „verbergen", „separieren" und „abstrahieren" sowie prozessorientierte Strategien wie „informieren", „kontrollieren", „durchsetzen" und „demonstrieren" umgesetzt.[52]

Auf Grundlage dieser Privacy Design Strategien können die vom EDPB geforderten Zielvorgaben beim Einsatz der JENTIS DCP bei entsprechender Konfiguration vollständig umgesetzt werden:

aa) Transparency

(1) Zur Erfüllung der Zielvorgabe „Transparenz" soll die betroffene Person in die Lage versetzt werden, nachzuvollziehen, wie personenbezogene Daten verarbeitet werden, sodass sie ihre Rechte nach Art. 15 bis 22 DSGVO verstehen und ausüben kann.[53] In erster Linie wird der **Transparenzgrundsatz** durch leicht zugängliche und in verständlicher sowie in klarer und einfacher Sprache abgefasste **Datenschutzinformationen** nach Maßgabe von Art. 12-14 DSGVO **umgesetzt** (vgl. Erwägungsgrund 39 DSGVO).

(2) Die vom EDPB geforderten **Gestaltungs- und Voreinstellungselemente** für den Transparenzgrundsatz[54] können im Rahmen der JENTIS DCP vollständig abgebildet werden. Die Pflicht zur **Transparenz** nach der DSGVO findet demnach auf drei **Kernbereiche** Anwendung, die für die praktische Arbeit und das Design der JENTIS DCP von erheblicher Bedeutung sind:

- Die **Unterrichtung** der betroffenen Person an sich.

[48] EDPB, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260, rev.01, Anhang.
[49] Borking, Privacy-Enhancing Technologies: The Path to Anonymity.
[50] Cavoukian, Privacy by design: the definitive workshop.
[51] EDPB-Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
[52] Vgl. Agencia Espanola Proteccion Datos (AEPD), A Guide to Privacy by Design 2019, S. 23 f.
[53] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 15.
[54] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 15.

- Die **Art und Weise**, wie die Verantwortlichen mit den betroffenen Personen in Bezug auf ihre Rechte kommunizieren.
- Die Ermöglichung der **Ausübung der Betroffenenrechte**.

(3) Mithilfe der JENTIS DCP verfügen Website-Betreiber über die volle Kontrolle und Kenntnis der vom Endgerät der Nutzer erfassten und an Drittanbietersysteme weitergeleiteten Datenparameter. Daher können im Einklang mit Art. 12 ff. DSGVO die Informationspflichten und mit Art. 15 ff. DSGVO die Betroffenenrechte vollständig erfüllt werden.

bb) Lawfulness

(1) Der Verarbeitung personenbezogener Daten muss eine gültige Rechtsgrundlage zugrunde liegen (Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 DSGVO). Die getroffenen Maßnahmen und Garantien sollen sicherstellen, dass der gesamte Verarbeitungszyklus mit der Rechtsgrundlage in Einklang steht. Die vom EDPB geforderten **Gestaltungs- und Voreinstellungselemente** für den Rechtmäßigkeitsgrundsatz[55] können im Rahmen der JENTIS DCP vollständig abgebildet werden.

(2) In Abhängigkeit der jeweiligen Verarbeitungsphase, der Nutzung bestimmter Identifier und der jeweiligen Use Cases kommen je nachdem, ob es sich um einen unmittelbaren Endgerätezugriff (vgl. dazu bereits **Pkt. I.2. und I.3.**) oder um eine nachgelagerte Verarbeitungsphase (vgl. dazu bereits **Pkt. I.4.**) handelt, unterschiedliche Rechtsgrundlagen für die Verarbeitung bei Nutzung von „JENTIS DCP“ in Betracht.

(3) Sofern für Use Cases Machine-Learning-Algorithmen verwendet werden, liegt überdies keine automatisierte Entscheidung im Einzelfall i. S. d. Art. 22 Abs. 1 DSGVO vor, da es aufgrund der Vermeidung unmittelbarer Zugriffe von Drittanbietersystemen zu keiner signifikanten Beeinträchtigung der Grundrechte betroffener Personen kommt.

cc) Purpose Limitation

(1) Als weiteres **Leitmotiv** von Privacy by Design und Default ermöglicht die JENTIS DCP die Einhaltung des in Art. 5 Abs. 1 lit. a) DSGVO normierten **Zweckbindungsgrundsatzes**, sollten Kundendaten aus z. B. CRM-Systemen nach spezifischer Kundenkonfiguration in Abweichung der Standardeinstellungen für die Anbindung von Audiences Tools über den JENTIS Tool Connector verwendet werden.

(2) **JENTIS** verfolgt keine eigenen Zwecke, sondern verarbeitet sämtliche Daten auf Weisung nach erfolgter Konfiguration des JENTIS DCP durch die Website-Betreiber, die im Auftragsdatenverarbeitungsvertrag sowie in den Konfigurationseinstellungen dokumentiert sind.

(3) Mithilfe der JENTIS DCP können Website-Betreiber die notwendige Zweckkompatibilität nach Art. 6 Abs. 4 DSGVO gewährleisten.

[55] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 16.

dd) Fairness

(1) Die Pflicht zur **Fairness** nach der DSGVO (Art. 5 Abs. 1 lit. a) DSGVO) wird nach Ansicht des EDPB unter anderem durch Umsetzung folgender **Kernelemente** erfüllt, die für die praktische Arbeit und das Design der JENTIS DCP von erheblicher Bedeutung und nicht durch andere Zielvorgaben abgedeckt sind[56]:

- Sicherstellung der Autonomie und Interaktion durch Einbeziehung betroffener Personen über die Verwendung der Daten sowie klare Kommunikation zur Wahrnehmung der Betroffenenrechte;
- Sicherstellung von „Truthfulness" durch Vermeidung von abredewidrigen und irreführenden Verarbeitungen;
- Keine Diskriminierung von Nutzern durch Verwendung diskriminierender Segmente sowie
- Verwendung fairer Algorithmen zur Reduzierung algorithmischer Verzerrungen und Transparenz gegenüber Betroffenen.

Die **JENTIS DCP** wurde designed, um eine faire Verarbeitung zu gewährleisten.

Der Einsatz der JENTIS DCP ermöglicht die **vollständige Umsetzung** von Betroffenenrechten wie Auskunftsanfragen, Löschungsersuchen und Widersprüchen gegen die Verarbeitung, indem sichergestellt wird, dass die Websitebetreiber die volle Kontrolle über die Datenverarbeitung haben.

Nach Ausübung einer der Optionen durch betroffene Personen und Mitteilung der Anfrage an JENTIS kann die JENTIS DCP vollautomatisiert im Namen und auf Wunsch der Kunden die Betroffenenrechte umsetzen.

(2) Zur Vermeidung **diskriminierender Schlussfolgerungen** aufgrund **algorithmischer Verzerrungen („algorithmic bias")**, also wenn Computersysteme die implizierten Werte und Vorurteile von Menschen – etwa bei Zuordnung von Nutzern zu unzutreffenden Segmenten – widerspiegeln,[57] hat JENTIS eine Evaluation der Machine-Learning-Modelle für die spätere Bildung z.B. von Synthetic User in Anlehnung an ein „Algorithm Audit" durchgeführt.

Jenseits möglicher algorithmischer Verzerrungen, die auf Programmierungsfehler zurückzuführen sein können, sind auf Grundlage der **Produktbeschreibung keine diskriminierenden Faktoren** zu erkennen.

ee) Data Minimisation

(1) Die **Kernelemente** des Grundsatzes der Datenminimierung als Zielvorgabe für Privacy by Design and Privacy by Default können im Rahmen der JENTIS DCP vollständig **umgesetzt** werden. Hierzu zählen laut EDPB[58] unter anderem:

- Datenvermeidung und -begrenzung,
- Zugriffsbeschränkungen auf Datensätze,
- Datenrelevanz und Erforderlichkeit der Daten in Relation zum Verarbeitungszweck,
- Aggregation sowie
- Pseudonymisierung nach dem Stand der Technik.

---

[56] Vgl. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 18.
[57] Vgl. Spindler/Horváth, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl., Art. 22 DSGVO Rn. 8; Herberger, NJW 2018, 2825, 2827.
[58] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 21.

(2) Abgesehen von der Möglichkeit einer **validen Pseudonymisierung** von Klardaten auf Rohdatenebene (vgl. Pkt. I.3. und 4.) und **umfassenden Zugriffsbeschränkungen**, die durch Konfiguration der JENTIS DCP sichergestellt werden kann, werden Nutzerdaten z.B. bei erweiterten Anwendungen wie dem Synthetischer User und ID-Pooling **aggregiert**.

(3) Die Speicherdauer der Rohdaten kann individuell festgelegt werden. In der Standardkonfiguration beträgt die Speicherdauer der Rohdaten 10 Tage.

Ebenso lässt sich für den JENTIS Tracker die Laufzeit der JENTIS Cookies im First-Party-Kontext kundenspezifisch konfigurieren. Über die JENTIS Server Suite können Datenparameter auf ein Mindestmaß reduziert oder modifiziert werden, um die Einhaltung des Datenminimierungsgrundsatzes je nach Einsatzzweck zu gewährleisten.

ff) Accuracy and Storage Limitation

(1) Die weiteren Zielvorgaben der Datenrichtigkeit und Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. d) und e) DSGVO[59] können Website-Betreiber aufgrund der **flexiblen Konfigurationsmöglichkeiten** der JENTIS DCP vollständig **umsetzen**.

(2) Die Kunden entscheiden, welche Daten über die JENTIS DCP erfasst und über den JENTIS Tool Connector in Drittanbieter-Systemen eingespeist werden, und können die Speicherdauer frei festlegen.

gg) Integrity and Confidentiality

(1) Die Sicherstellung der Anforderungen an die Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO) als Zielvorgabe von Privacy by Design und Privacy by Default ist eines der **Kernprinzipien** in JENTIS SaaS.

(2) Durch Implementierung von angemessenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik wie die Pseudonymisierung und Verschlüsselung stellt JENTIS die Sicherheit der Verarbeitung (Art. 32 DSGVO) sicher. Außerdem ermöglicht die Bereitstellung der JENTIS DCP unter Verwendung der Serverstruktur von IONOS die Umsetzung der Datenseparierung, Abschirmung von äußeren Einflüssen und die Verarbeitung in einem logisch isolierten virtuellen Netzwerk innerhalb der Cloud-Infrastruktur.

(3) In der **Anlage** zum **Auftragsverarbeitungsvertrag** können die jeweils aktuellen **technischen und organisatorischen Maßnahme**n von JENTIS und von IONOS eingesehen werden.

JENTIS wendet ein Information Security Managementsystem in Übereinstimmung mit der **ISO 27001:2023** an. In Übereinstimmung mit den Verfahren der TV AUSTRIA wird bescheinigt, dass JENTIS ein Managementsystem in Übereinstimmung mit der oben genannten Norm für den folgenden Geltungsbereich anwendet: Die Erbringung von Dienstleistungen im Bereich der Datenerfassung auf Websites und aus anderen digitalen Datenquellen unter Verwendung von JENTIS-Technologien.

[59] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default v2.0, S. 23 ff.

hh) Accountability

Die umfangreiche Rechenschaftspflicht für Verantwortliche in Art. 5 Abs. 2 DSGVO nach Maßgabe der EuGH-Rechtsprechung führt dazu,[60] dass Website-Betreiber den Entscheidungspfad zur Konfiguration der JENTIS DCP vollständig dokumentieren und vorlegen sollten, um die Einhaltung von Art. 25 DSGVO im Falle streitiger Auseinandersetzungen beweisen zu können. Die JENTIS-UI (User Interface) ermöglicht es Website-Betreibern, dieser Rechenschaftspflicht zu erfüllen.

2. TCF-Compliance

Bei dem Einsatz der JENTIS DCP ist die Compliance mit dem Transparency and Consent Framework **(TCF v2.2) sichergestellt**. Mithilfe der JENTIS DCP können alle vendorspezifischen Anforderungen aus der IAB TCF Policy[61] erfüllt werden.

3. "Schrems II"-Compliance für Drittlandübermittlungen

(1) Für den Fall, dass ein **Analysedienst aus den USA** wie Google Analytics eingebunden wird, kann der Drittlandtransfer an die Google LLC aufgrund der aktiven Zertifizierung[62] der Google LLC unter der Data Privacy Framework List[63] auf den Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023[64] gestützt werden.

(2) Soweit ein **Datentransfer** nach **Indien, China oder Russland** aufgrund des Einsatzes z. B. von Google DV 360[65] stattfindet und nicht auf einen Angemessenheitsbeschluss der EU-Kommission[66] gestützt werden kann, da für Datentransfers für Indien, China oder Russland ein solcher nicht existiert, bedarf es einer zusätzlichen Absicherung des Drittlandtransfers. Der EDSA stuft Indien im Rahmen einer in Auftrag gegebenen Studie[67] als Drittland ohne angemessenes Schutzniveau ein, insbesondere mit Blick auf die geheimdienstlichen Befugnisse von Sicherheitsbehörden.

Gleiches gilt, wenn lediglich Analysedienste mit Sitz in den USA eingesetzt werden, die jedoch keine aktive Zertifizierung unter der Data Privacy Framework List[68] aufweisen; auch insofern bedarf es einer weiteren Rechtfertigung eines Drittlandtransfers, weil der Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023[69] dann keine Anwendung findet.

(3) Selbst mittels einer **Standortwahl** von **Servern** in **Europa** lässt sich die **Drittlandthematik nicht** von vornherein **vermeiden**, wie das OLG Köln kürzlich für die Nutzung von Google Ads mit Serverstandort in der EU bestätigt hat.[70]

---

[60] EuGH, Urt. v. 27.10.2022 – C-129/21, Rn. 80 f.
[61] IAB Europe Transparency & Consent Framework Policies.
[62] U.S. Department of Commerce, Data Privacy Framework List.
[63] U.S. Department of Commerce, Data Privacy Framework List.
[64] Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023
[65] Vgl. https://www.iccl.ie/digital-data/europes-hidden-security-crisis/.
[66] Angemessenheitsbeschlüsse der EU-Kommission.
[67] Czarnocki et al., Government access to data in third countries.
[68] U.S. Department of Commerce, Data Privacy Framework List.
[69] Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023.
[70] OLG Köln, Urt. v. 03.11.2023 – 6 U 58/23; ebenso Gutachten im Auftrag der DSK zum aktuellen Stand des US-Überwachungsrechts zur Anwendung von US-Überwachungsgesetz 50 U.S. Code § 1881a (Section 702 FISA) sowie Heckmann, Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern, Wissenschaftliches Gutachten, 2021, S. 16.

(4) Die Abfrage einer **ausdrücklichen Einwilligung** nach Art. 49 Abs. 1 lit. a) DSGVO für den **Drittlandtransfer** im Einwilligungsdialog oder in den Datenschutzinformationen ist von der Einwilligung in den Einsatz von Tracking-Tools zur Nachverfolgung des Nutzerverhaltens nach Ansicht der **DSK** zu unterscheiden und kann durch diese nicht ersetzt werden.[71] Umfang und Regelmäßigkeit solcher Transfers widersprächen regelmäßig dem Charakter des Art. 49 DSGVO als Ausnahmevorschrift und den Anforderungen aus Art. 44 S. 2 DSGVO.[72]

Außerdem wurde vom OLG Köln ein allgemeiner Hinweis im Cookie-Banner einer Website, dass das Datenschutzniveau in den USA nicht mit dem in der EU gleichwertig sei, als unzureichend erachtet.[73]

(5) Aufgrund der Anforderungen der EuGH-Rechtsprechung[74] an den Drittlandtransfer verbleibt praktisch nur die Vereinbarung von Standardvertragsklauseln[75] (SCC). Die Absicherung des Drittlandtransfers über **Standardvertragsklauseln** („**SCC**“, Art. 46 Abs. 2 lit. c) DSGVO) bedarf jedoch zusätzlicher Maßnahmen **(„Supplementary Measures“)**.

Welche „**Supplementary Measures**“ zu ergreifen sind, ist anhand der vom **EDPB** am 18.06.2021 im Nachgang zu den neuen SCC der EU-Kommission veröffentlichten „Recommendations 01/2020 on measures […]”[76] in der Version 2.0 zu evaluieren. Ohne Dokumentation von zusätzlichen Maßnahmen zur Riskmitigation wird die Anwendung der SCC von Aufsichtsbehörden nicht akzeptiert. Als **Zusatzmaßnahmen** können z. B. die **Anonymisierung** oder fortgeschrittene **Pseudonymisierung** von Daten sowie weitgehende **Verschlüsselungstechnologien** in Betracht kommen, wenn sichergestellt ist, dass die Empfänger im Drittland keinen Zugriff auf die Zuordnungsregel für die pseudonymisierten Daten i. S. d. Art. 4 Nr. 5 DSGVO oder die zu verarbeitenden Daten erhalten.[77]

Das **OLG Köln** und das **BVwG** (Österreich) haben übereinstimmend die **Kürzung von IP-Adressen**, eine dem Stand der Technik entsprechende **Verschlüsselung in transit sowie** eine Verschlüsselung **at rest** für **nicht ausreichend** erachtet.[78] Die europäischen **Aufsichtsbehörden** stellen an **Zusatzmaßnahmen** beim nicht modifizierten Einsatz von Tracking-Diensten von US-Anbietern **strenge Anforderungen**.

Nach Ziff. 14 der von der EU-Kommission bereitgestellten Standardvertragsklauseln[79] ist eine Pflicht zur Durchführung und Dokumentation eines „**Transfer Impact Assessments**“ vorgesehen, in dem eine Analyse und Mitigation der Risiken eines Zugriffs von Sicherheitsbehörden auf Grundlage von „Additional Measures“ als zusätzliche vertragliche, technische und organisatorische Maßnahmen zu erfolgen hat.

Mithilfe der JENTIS Server Suite können Datenparameter auf das Mindestmaß reduziert, modifiziert oder synthetisiert werden. Laut **EDPS** können „**synthetische Daten**“ als Technologie zur Verbesserung des Schutzes der Privatsphäre (**Privacy Enhancing Technology**) als „Additional Measure“ zur Absicherung von Drittlandtransfers betrachtet werden.[80] Die Synthetisierung dient nach Ansicht der **ENISA** in erster Linie der

[71] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 32.
[72] Vgl. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 vom 25.5.2018, S. 9.
[73] OLG Köln, Urt. v. 03.11.2023 – 6 U 58/23.
[74] EuGH, 16.7.2020 – C-311/18 – Schrems II.
[75] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679.
[76] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
[77] Paal/Kumkar, MMR 2020, 733.
[78] OLG Köln, Urt. v. 03.11.2023 – 6 U 58/23; BVwG, Entsch. v. 12.05.2023 W245 2252208-1/36E.
[79] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679.
[80] EDPS, techsonar 2021-2022, S. 10.

Vertraulichkeit der **Verarbeitung**,[81] die den Charakter „zusätzlicher Maßnahmen" in technischer und organisatorischer Hinsicht i .S. d. Art. 32 DSGVO aufweist.

Sofern SCC abgeschlossen werden, müsste in inhaltlicher Hinsicht sichergestellt werden, dass in Anhang II der SCC diese zusätzlichen vertraglichen, technischen und organisatorischen Maßnahmen hinreichend dokumentiert werden, die im Rahmen eines Transfer Impact Assessments evaluiert wurden.

III. Best Practices für Website-Betreiber

Zusammenfassend sind für den datenschutzrechtskonformen Einsatz der JENTIS DCP folgende Handlungsempfehlungen umzusetzen:

☐ **Kein Laden** der Tags von **Drittanbietern** als Auslöser des Endgerätezugriffs **vor Erteilung** einer **Einwilligungserklärung**

☐ Anpassung der **Abfrage** einer **Einwilligungserklärung** in Bezug auf die Analysetools sowohl für die endgerätebezogene Verarbeitung als auch für die nachgelagerte Analyse der Tracking-Daten

- Der Einwilligungsdialog mit den Nutzern der App sollte **folgende Informationen** nach Maßgabe der Rechtsprechung und Aufsichtsbehörden enthalten:
  - ErwGr. 42 S. 4 DSGVO: Identität des Verantwortlichen und Verarbeitungszwecke
  - EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 72 ff.[82]: Funktion, Dauer, Empfänger
  - EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679[83]: Identität, Zwecke, Datenkategorien, Widerruf, Empfänger, Drittlandtransfer
- Es empfiehlt sich, **keine Standardtexte** zu verwenden, sondern **konkrete Beschreibungen** der Verarbeitungsvorgänge der Einwilligungserklärungen in die CMP zu integrieren. Hierzu zählen nach den Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des EDSA[84] auch Angaben zur Verarbeitung mit **gemeinsam Verantwortlichen**.
- Hierfür können die Informationen auf unterschiedlichen Ebenen in der CMP eingeblendet werden, wobei die wesentlichen Informationen auf der ersten Ebene bereitgehalten werden müssen.[85]
- Nach einhelliger Ansicht in Rechtsprechung und aufsichtsbehördlichen Stellungnahmen bedarf es zur Erfüllung des Kriteriums der Freiwilligkeit der Einwilligung (Art. 4 Nr. 11 DSGVO) eines **gleichwertigen Ablehnungs-Buttons** auf der ersten Ebene der CMP.[86]
- Bei der Konfiguration der CMP ist sicherzustellen, dass zum Nachweis einer Einwilligung (Art. 7 Abs. 1 DSGVO) **keine langfristig gespeicherte ID** dem Endgerät der App-Nutzer zugeordnet wird.[87]
- Schließlich ist eine jederzeitige **Widerrufsmöglichkeit** einer bereits erteilten Einwilligung (Art. 7 Abs. 3 DSGVO) sicherzustellen. Diese kann durch Verlinkung der CMP-Einstellungen in den Datenschutzhinweisen oder App-Einstellungen realisiert werden.

---

[81] Vgl. ENISA, Data Protection Engineering, 2022, S. 17.
[82] EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 72 ff.
[83] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679.
[84] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679.
[85] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, Rn. 36.
[86] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, Rn. 132 ff; OLG Köln, Urt. v. 19.01.2024 – 6 U 80/23; LG München, Urt. v. 29.11.2022 – 33 O 14776/19, LG Berlin, 52 O 79/22 (2).
[87] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2022, Rn. 79.

- ☐ Für Weitergabe substituierter Datenströme an Drittanbietersysteme sowie bei Konfiguration der JENTIS DCP mit aktiviertem Feature JENTIS Essential Mode **Durchführung** eines **Legitimate Interests Assessment** zur Dokumentation der Interessenabwägung nach Maßgabe von Art. 6 Abs. 1 lit. f) DSGVO.
- ☐ **Abschluss Auftragsverarbeitungsvertrag mit JENTIS**
- ☐ **Anpassung Datenschutzerklärung auf der Betreiber Website**
- ☐ Zur Rechtfertigung des Drittlandtransfers: Anforderung von Dokumentationen der Drittpartei zur **Überprüfung** des **Abschlusses** der **Standardvertragsklauseln** mit Drittanbietern sowie **Durchführung** eines dokumentierten **Transfer Impact Assessments** im Einklang mit Ziff. 14 der Standardvertragsklauseln.

Anhänge:

- Product Description Ver6 as of 17.06.24
- JENTIS SYSTEM Diagram

Product Description

JENTIS Software as a Service

JENTIS Data Capture Platform

The JENTIS Data Capture Platform is a fully managed hosted, multi-component, server-side tracking technology that helps marketing teams capture high-quality, actionable first-party data. With privacy by design and configuration options, it addresses regulatory constraints, solves multi-device customer journeys, prevents loss of data due to ad-blockers and tracking protection mechanisms.

JENTIS Data Capture Platform simplifies data management, enhances budget allocation, increases campaign profitability and improves marketing campaigns' ROI.

At the heart of the JENTIS Data Capture Platform (JENTIS DCP) is the Tag Manager, which manages the components and orchestrates streaming data to the various third-party advertising and marketing systems. Via an easy to use administration UI, customers are able to independently manage the whole tagging and compliance process. From managing consent, tags, functions, triggers and states, through to the data destinations, customers are in complete control of their company's server-side tagging.

Product Description uses the following **Definitions**:

Account refers to a customer's profile within JENTIS SaaS. The customer ("Account owner") creates an Account, defines an Admin, and manages other Account users within it. Within an Account, containers are created to organize and manage data capture activities.

Container is a component within an Account that is associated with a specific domain. It hosts all the consents, vendors, tools, and tags for that domain. Multiple containers can be created per Account, but each container is dedicated to a single domain (*see **JENTIS Container Manager***).

Consent configuration refers to the settings managed by the Account owner to control consents for each Container. This includes configuring consent for each vendor, tool, and tag within the Container (*see **JENTIS Consent Manager***).

Vendor is a third-party destination where the Account owner sends data. Consent settings can be configured at the vendor level.

Tool sets the criteria for sending data to a vendor based on consent decisions of a data subject, data substitutions, and / or even specific campaign goals. The Account owner configures tools to handle different tracking scenarios.

Trigger defines when to send data to a destination. The Account owner configures triggers to determine the specific conditions and timing for data transmission.

Tag configuration involves assigning one or multiple tags to each Tool. These tags correspond to specific data subject interactions, enabling the Account owner to align data transmission in specific Tools with appropriate consent permissions (*see* ***JENTIS Tag Manager***).

The **core components** of the JENTIS DCP are as follows:

JENTIS Container Manager

The JENTIS Container Manager allows teams to operate within a single Container environment using the JENTIS Tag Manager and other components of the JENTIS SaaS.

The Account owner can manage different versions of a Container, including commenting, previewing, debugging, rolling back to previous versions, and publishing to stage and live environments. This aligns with industry best practices for efficient and organized data management.

JENTIS Consent Manager

The JENTIS Consent Manager is where the teams store information about data subject consents, as well as administer Consent Management Platforms (CMP) connectors with information from Vendors and Tools.

JENTIS Consent Manager makes it possible to connect native third-party CMPs, ensuring that all consents given by the CMP are available, documented and used based on the applicable consent configuration. JENTIS Consent Manager includes a JENTIS Essential Mode feature enabling an Account owner to configure different scenarios of tracking based on the consent decision of the data subject.

JENTIS Tag Manager

The JENTIS Tag Manager provides for a single location to easily add, update, or remove tags, states, triggers, variables and custom java script code for tracking data in the first-party

context, as well as other tracking data, in alignment with data subject consents based on various website events in a centralized and tidy user-friendly interface .

JENTIS Tool Connector

The JENTIS Tool Connector manages the 100+ out of the box connectors that send data to third party marketing and analytics Vendors that JENTIS supports. Account owners are able to easily create and connect Tools for various Vendors, such as Google Analytics, Meta, Tik-Tok, etc, and stream data to the Tool in accordance with a data subjects' consent based on the applicable Consent configuration.

JENTIS Tracker

The Account collects client side tags and first-party data based on the configurations in the JENTIS Tracker. JENTIS Tracker is then pushing this data to the server-side via the JENTIS Server Suite.

JENTIS Server Suite

JENTIS Server Suite (or J-Suite) is the backbone and the engine of the JENTIS SaaS. JENTIS processes the data on behalf of the Account. With the standard and advanced features of the J-Suite enabled, teams can modify the data (anonymize and pseudonymize), enrich and/or synthesize the data before they share it with vendors. The J-Suite is based on the Twin Server Technology.

JENTIS Twin Server

The JENTIS Twin Server is an integral part of the J-Suite and this is where the data is being processed, enriched and from where the data is streamed to vendors such as Google Analytics.

JENTIS DCP offers the following **additional and advanced features**:

JENTIS Synthetic User

In a scenario when a user consent is not provided, JENTIS relies on machine learning models to impute users' behavior and then combine real and synthetic users for improved marketing and analytics datasets.

JENTIS ID Pooling

ID Pooling uses pseudonymised user IDs to serve users with personalized content and run marketing campaigns in a privacy-compliant way. Our solution makes it possible to respect users' privacy while delivering personalized experiences.

JENTIS Data Enrichment

Connects to third-party APIs that provide real time enriched data for online marketing and analytics. This enables companies to add commercially sensitive or other attributes to the data that is streamed to Vendors, such as Google Analytics.

JENTIS Raw Data Tool

The JENTIS Raw Data Tool enables the download of JENTIS raw data for advanced analytics and ML/AI modeling needs. Teams also benefit from full data sovereignty and vendor independence.

JENTIS SYSTEM Diagram